谨防诈骗

骗子经常会伪装成 Services Australia 等具有公信力的机构行骗。

骗子可能会以提供福利金、服务和帮助等名义诱骗受害者的金钱或个人信息。

一旦骗取了你的个人信息，骗子就可以：

- 访问你的银行账户并将账户中的钱款转移
- 冒用你的姓名签订电话合约和其他合同
- 偷取你的退休公积金
- 访问你的电子邮件和社交媒体账户
- 冒用你的身份。

一旦钱财被骗，就可能无法找回。

骗子企图获取的信息

骗子可能会试图骗取你的：

- 全名
- 出生日期
- 地址
- Medicare 卡信息
- Centrelink Customer Reference Number (CRN)
- 身份证件
- myGov 登录信息或链接码
- 银行账户详情
- 密码。

如何保护自己

要保护好个人信息，就要：

- 懂得如何识别骗局
- 如果某人突然联系你，则要提高警惕，特别是涉及某种紧急截止日期的事情
- 不要将链接代码、密码或安全问题的答案告诉任何人
- 不要让他人使用或看到你的 myGov 或其他在线账户
- 使用自己容易记住，但别人很难猜到的密码
- 移动设备在不使用时，要加以锁定保护
- 确保邮件的安全——在信箱上加一把锁；如果搬家，则安排邮件转递服务。

如何识别骗局

可通过了解我们会做什么和不会做什么来识别骗局。

我们会做的事情

我们可能向你发送电子邮件或短信。我们的信息不会包括你的姓名或联系信息，但可能会：

- 要求你进行预约，或提醒你进行预约
- 告知有关福利金领取的情况
- 确认你详情的变更
- 通知你的 myGov 收件箱里有新的信息。

如果你有欠款，我们会寄信通知。

我们可能会给你打电话，但如果是突然接到我们的来电，则请小心。应问清楚来电者的姓名和联系方式。如果认为打电话的人不是我们，则请挂断电话，然后回拨我们的福利金事务专线。

我们不会做的事情

我们**绝不会**要求你：

- 告诉我们你的密码或 Personal Identification Number (PIN)
- 付钱给我们以换取帮助
- 寄钱或转钱给我们，以获得福利金
- 购买礼品卡或代金券
- 点击电子邮件或文本信息中的链接或打开附件
- 在社交媒体上向我们提供你的个人资料，如 Facebook 或 Twitter
- 让我们访问你的电脑或个人设备。

我们也不与其他公司合作，为你提供特殊优惠。

如果遭到了诈骗该怎么办

如果损失了钱财或泄露了个人信息，则应该：

- 记下所发生的事情
- 请立即致电我们的 Scams and Identity Theft Helpdesk，电话是 **1800 941 126**。如果需要口译服务，请告诉我们，我们将免费安排口译员。
- 访问 **scamwatch.gov.au** 网站，用英语报告诈骗事件

更多信息

- 致电 **131 202**，用中文咨询 Centrelink 相关福利金和服务的信息
- 致电 **131 450**，联系 Translating and Interpreting Service (TIS National)，用中文咨询 Medicare 和 Child Support 相关福利金和服务的信息

- 请浏览 **servicesaustralia.gov.au/yourlanguage** 获得中文版的文本、音频或视频信息
- 请浏览 **servicesaustralia.gov.au/scams** 了解更多英文信息
- 前往 Centrelink 服务中心。

注意：从澳大利亚任何地方用座机拨打“13” 打头的电话号码，费用固定。该费率可能因本地通话价格而异，也可能因电话服务提供商而异。使用座机拨打“1800”开头的电话号码免费。使用公共电话和移动电话致电可能会以较高的费率按时计费。

免责声明：

本出版物中包含的信息仅作为福利金和服务指南之用。你有责任决定是否要申请某项福利金，并根据个人具体情况提出申请。

Beware of scams

Scammers often pretend to be from trusted organisations, like Services Australia.

They may trick you into giving away money or information in return for payments, services and help.

If a scammer gets your information, they can:

- access your bank account and transfer money from it
- use your name to set up a phone plan and other contracts
- steal your superannuation
- access your email and social media accounts
- pretend to be you.

If you lose money because of a scam, you may not get it back.

Information scammers want

Scammers may try to get your:

- full name
- date of birth
- address
- Medicare card details
- Centrelink Customer Reference Number (CRN)
- identity documents
- myGov sign in details or linking codes
- bank details
- passwords.

How to protect yourself

To protect your information:

- know how to identify a scam
- be careful when someone unexpectedly contacts you, especially if they have an urgent deadline
- never tell anyone your linking codes, passwords or answers to your secret questions
- do not let others use or see your myGov, or other online accounts
- use a password that is easy for you to remember, but hard for others to guess
- protect your mobile device by locking it when you are not using it
- secure your mail by having a lock on your letterbox and redirecting your mail if you move.

How to tell if it is a scam

You can identify a scam by knowing what we do and what we do not do.

Things we do

We may send you an email or text message. Our messages will not include your name or contact details, but may:

- ask you to book, or remind you about, an appointment
- tell you about your payments
- confirm when you have changed your details
- tell you if you have a new message in your myGov Inbox.

If you owe us money, we will send you a letter.

We may call you, but be careful if you are not expecting a phone call from us. You should ask for the caller's name and contact details. If you do not think the caller is us, hang up and call back on one of our payment lines.

Things we do not do

We will **never** ask you to:

- tell us your password or Personal Identification Number (PIN)
- pay us to help you
- send or transfer money to us to get a payment
- buy gift cards or vouchers
- click on links or open attachments in emails or text messages
- give us your personal details on social media, like Facebook or Twitter
- give us access to your computer or personal devices.

We also do not work with other companies to give you special deals.

What to do if you have been scammed

If you have lost money or given away personal information, you should:

- keep a record of what happened
- call our Scams and Identity Theft Helpdesk straight away on **1800 941 126**. Let us know if you need an interpreter and we will arrange one for free.
- report the incident in English at **scamwatch.gov.au**

Where to get more information

- call **131 202** to speak with us in your language about Centrelink payments and services
- call the Translating and Interpreting Service (TIS National) on **131 450** to speak with us in your language about Medicare and Child Support payments and services

- go to **servicesaustralia.gov.au/yourlanguage** where you can read, listen to or watch information in your language
- go to **servicesaustralia.gov.au/scams** for more information in English
- visit a service centre.

Note: calls from your home phone to ‘13’ numbers from anywhere in Australia are charged at a fixed rate. That rate may vary from the price of a local call and may also vary between telephone service providers. Calls to ‘1800’ numbers from your home phone are free. Calls from public and mobile phones may be timed and charged at a higher rate.

Disclaimer

The information contained in this publication is intended only as a guide to payments and services. It’s your responsibility to decide if you wish to apply for a payment and to make an application with regard to your particular circumstances.